8

5

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/818,914	03/26/2001	W. Dale Hopkins	20206-16 (P00-3324)	4267

25696 7590 10/06/2004

OPPENHEIMER WOLFF & DONNELLY
P. O. BOX 10356
PALO ALTO, CA 94303

EXAMINER
CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/818,914	**Applicant(s)** HOPKINS
	Examiner Paul Callahan	**Art Unit** 2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2001*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-63* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-63* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2001* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *09142004*.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-63 are pending in this application and have been examined.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 USC 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1, 2, 5, 6, 7, 9-11, 15, 17, 20, 24, 27, 28, 30, 36, 37, 39, 41, 45, 47, 49, 53-55, and 57-62 are rejected under 35 USC 112 second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which the applicant regards as the invention.

The claims each contain the phrase: "substantially simultaneously" It is not clear what is meant by "substantially" in this context.

Claims 3, 4, 8, 12-14,16, 18, 19, 21-23, 25, 26, 29, 31-35, 38, 40, 42-44, 46, 48, 50-52, 56, and 63 are dependent on the rejected claims and are thereby rejected on the same basis.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1, 12, 13, 14, 28, 29, 31, 32, 34, 54, and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over Handbook of Applied Cryptography, Menezes et al., CRC Press 1996, pages 134-168, and Quisquater et al., "Fast Decipherment Algorithm for RSA Public Key Cryptosystem," Oct. 1982, Electronic Letters, Vol. 19, No. 21.

As for claims 1, Menezes teaches a process of searching for a plurality of prime number values, comprising the steps of: randomly generating a plurality of k random odd numbers each providing a prime number candidate (Sec. 4.1.1, p. 134); and performing at least one primality test on each of said candidates (Sec. 4.1.1, p. 134), each of said primality tests including an associated exponentiation operation (Sec. 4.2.3 p. 138-140).

Menezes does not teach a processing system including a processing unit and a plurality of exponentiation units communicatively coupled to the processing unit, or that the primality tests are carried out by the plurality of exponentiation units in parallel and where the exponentiation operations are carried out substantially simultaneously. However Quisquater et al, teaches such a parallel arrangement of exponentiators (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 12, Menezes teaches a step of performing at least one primality test that includes performing a Fermat type primality test (Sec. 4.2.1).

As for claim 13, Menezes teaches a step of performing at least one primality test that includes performing a Miller-Rabin type primality test (Sec. 4.2.3).

As for claim 14, Menezes teaches a step of randomly generating a plurality of k random odd numbers that further includes: defining a length L for each of the plurality of k random numbers to be generated; and generating each of said plurality of k random odd numbers in an interval between 2L and 2L-1 (Sec. 4.4.3).

As for claim 28, Menezes teaches a prime number generating process of searching in parallel for a plurality of prime number values, comprising the steps of randomly generating a plurality of k :random odd numbers expressed as no,o, nl,o, . n((k-1)),0, each said number providing a prime number candidate; determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers no,o, nl,o, n(k-1),O to provide (k X y) additional prime number candidates (no,,, 110,2, no,y), (nl,l, n1,2, n1,y), . (n(k-1),1, n(k-1),2, n(k-1);,) thereby yielding a total number of (k r (y+1)) prime number candidates (Page 148, Sec. 4.5.1); sieving said (k x (y+1)) prime number candidates by performing a small divisor test on each of said candidates in order to eliminate candidates revealed to be composite numbers by said small divisor test thereby yielding a sieved number s of candidates (Page 145, Sec. 4.4.1); and performing at least one primality test on each of said sieved number s of candidates (Page 148, Sec. 4.5.1), each of the plurality of s primality tests including an associated exponentiation operation (Page 146, Sec 4.4.1). Menezes does not teach the exponentiation operations being executed by an associated one of a plurality of the exponentiation units, where the exponentiation operations are performed by a plurality of exponentiation units substantially simultaneously. However Quisquater does teach such an arrangement of parallel exponentiators, (fig. 1, page 2 paragraph 7). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the method of Menezes. It would have been desirable to do so as this would allow for computation to proceed more rapidly. The motivation to make this combination is found for example, in Menezes Sec. 4.1 Introduction where the efficiency of generation of public key parameters in public key systems such as RSA is discussed.

As for claim 29 and 34, Menezes teaches a prime number generating system as recited in wherein said step of determining a plurality of y additional odd numbers based on each one of the randomly generated odd numbers no,o, nl,o, .. . n(k-1),O includes successively adding two to each of said randomly generated odd numbers no,o, nl,o, . n(k-1),O to provide (k x y) additional prime number candidates expressed as (no,1= no,o+ 2 , no,2 -=no,o+ 4, . no,y = lio,o + (y-2)), (nl,l = n1,o+ 2 , n1,2= n1,o+ 4, n1,y = nl,o + (y-2)), . (n(k_1),1= n~k-1)>o+ 2 , n(k-1),2=n‘-k-1),o+ 4, n(k_1),y = n(k-1),O +(y.2)). (Page 148, Sec. 4.5.1).

As for claim 31, Menezes teaches a prime number generating system wherein said step of performing at least one primality test includes performing a Fermat type primality test. (Sec. 4.2.1).

As for claim 32, Menezes teaches a prime number generating system wherein said step of performing at least one primality test includes performing a Miller-Rabin type primality test. (Sec. 4.2.3).

As for claim 33, Menezes teaches a prime number generating system wherein said step of randomly generating a plurality of k random odd numbers further includes: defining a length L for each of the plurality of k random numbers to be generated; and generating each of said plurality of k: random odd numbers in an interval between 2L and 2L_1. (Sec. 4.4.3).

As for claims 54 and 57, the claims represent the computer program product embodied in a memory medium which when read out, causes the system of Claim 1 to carry out the process of generating prime numbers, and therefore is rejected on the same basis as claim 1.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. The following documents disclose method of generation of prime numbers similar to the applicant's invention:

Collins et al.	6,378,072
Dupaquis	6,718,536

Miller et al.	4,351,982
Itoh et al.	6,330,332
Matayas, Jr. et al.	6,345,098
Matayas, Jr. et al.	6,307,938
Hori	6,578,057

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (703) 305-1336. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Andrew Caldwell, can be reached on (703) 306-3036. The fax phone number for the organization where this application or proceeding is assigned is: (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

9/14/04

Paul Callahan